Outbank Helpdesk

Wie kann ich mich als Nutzer beim Banking im Netz schützen?

Krisztina - 2019-02-14 - in Datensicherheit

Links und Anhänge von E-Mails prüfen

Häufig schleusen sich Viren durch infizierte E-Mail-Anhänge oder -Links auf den PC oder das Smartphone. Diese Spoofing-Mails sind mittlerweile stark ausgereift: Sie passen sich dem Nutzer an und geben als Absender einen bekannten Namen oder eine Institution an, mit welchen der Nutzer häufig in Kontakt steht.
Daher solltest du keine Anhänge öffnen, deren Absender du nicht kennst. Wenn du bei einer E-Mail unsicher bist, kannst du eine kurze Google-Suche mit der Betreffzeile der E-Mail durchführen. Sollte es sich um eine infizierte Spam-Mail handeln, weisen meist bereits die ersten Suchergebnisse darauf hin.

Offizielle App Stores nutzen

Wer Apps nicht aus den offiziellen App Stores von Google oder Apple herunterlädt, läuft Gefahr, sein Gerät mit Viren zu infizieren. Gerade bei sehr beliebten Apps besteht die Gefahr, dass verseuchte Download-Links von diesen Versionen im Umlauf sind.
Du solltest deshalb Apps ausschließlich aus dem Apple App Store oder Google Play Store herunterladen. Alle Apps, die dort gelistet sind, werden von den jeweiligen Plattformen zuvor geprüft. Sie können deshalb in der Regel bedenkenlos heruntergeladen werden.

Authentifizierung mit 2 Geräten durchführen

Beim sicheren TAN-Verfahren kommen üblicherweise zwei, voneinander unabhängige Geräte zum Einsatz für die Zwei-Faktor-Authentisierung. Im photoTAN-Verfahren wird die TAN jedoch nicht auf einem zweiten Gerät generiert. Angreifer haben somit leichtes Spiel: Sie nisten sich über ein Schlupfloch im Smartphone ein und manipulieren die TAN-Generierung so, dass das Geld auf ein anderes Konto geleitet wird.
Aus diesem Grund solltest du stets zwei verschiedene Geräte für TAN-Verfahren verwenden. Bei einer Überweisung macht es beispielsweise Sinn, die mobile TAN für die Transaktion auf dem Smartphone zu empfangen und den Vorgang selbst am Mac oder PC durchzuführen.

Webseiten ohne Schloss vermeiden

Jede Webseite, die Nutzerdaten abfragt oder speichert, sollte über ein Sicherheitszertifikat verfügen. Dieses bescheinigt, dass die Datenströme verschlüsselt sind. Liegt kein Zertifikat vor, können die Daten unter Umständen frei eingesehen werden und bieten Angreifern ein einfaches Ziel.
Prüfe deshalb immer vor der Registrierung auf einer Webseite, ob in der URL-Leiste ein kleines Vorhängeschloss-Icon vorhanden ist. Wenn ja, ist eine Grundsicherheit geschaffen.

Auf Banking in öffentlichen Netzen verzichten

Im Gegensatz zum heimischen Privat-WLAN sind öffentliche WLAN-Verbindungen in den wenigsten Fällen verschlüsselt. Wer sich hier einloggt, läuft Gefahr, dass seine Daten abgefangen oder manipuliert werden. Teilweise richten Kriminelle sogar eigene “Free Wifi”-Verbindungen ein, nur um anschließend die verbundenen Geräte zu hacken und die Daten mitzulesen.

Im öffentlichen WLAN solltest du deshalb keine persönlichen oder vertraulichen Daten abrufen oder gar Mobile Banking nutzen. Surfst du häufig über fremde Rechner, solltest du anschließend immer den Cache des Browsers löschen. Werden diese Informationen nicht gelöscht, könnten Kriminelle diese später auslesen und missbrauchen.